COMMONWEALTH OF MASSACHUSETTS

DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

Investigation by the Department on its own motion, pursuant to G.L. c. 159 §§ 12 and 16, into the collocation security policies of Verizon New England Inc. d/b/a Verizon Massachusetts	D.T.E 02-8

PANEL REBUTTAL TESTIMONY OF QWEST COMMUNICATIONS CORPORATION

Members of Panel:

Michael Adragna
Anne Cullather

May 15, 2002

WITNESS OR WITNESS PANEL

Q. PLEASE IDENTIFY THE NAME AND BUSINESS ADDRESS OF THE INDIVIDUAL PANEL MEMBERS TESTIFYING ON BEHALF OF QWEST.

A. The members of this panel, in alphabetical order, are: Michael Adragna and Anne Cullather. Mr. Adragna's business address is 700 W Mineral Avenue, Room IDQ9, Littleton, Colorado 80120; and Ms. Cullather's business address is 4250 North Fairfax Drive, Arlington, Virginia 22203.

Q. PLEASE DESCRIBE THE CURRENT POSITION, EDUCATIONAL BACKGROUND AND PROFESSIONAL EXPERIENCE OF BOTH PANEL MEMBERS.

A. **Mr. Michael Adragna** is Senior Manager of Physical Security, and has been responsible for Qwest's physical security across the country since 1996. In that capacity, he develops access control methods and procedures, construction standards, and physical access control budget priority; issues and tracks picture identification badges which include card access, key management, access control system product selection, operations and maintenance of all physical security systems and contract administrator for the security officer contract. In this position, Mr. Adragna has attended conferences conducted by the American Society of Industrial Security and the International Security Conference, and has become familiar with endeavors of the Network Reliability and Interoperability Council, as well as the National Security Telecommunications Advisory Committee. Since September 11, 2001, he has focused on researching anti-terrorism construction standards for network buildings and conducted site assessments on existing premises.

Prior to his current position, he lead the real estate master planning team for the former U S West, and assisted its overseas affiliates, in developing construction

standards. Mr. Adragna obtained his construction project management certification from Denver University in 1986. He received his business degree from the University of Phoenix in 1993, and subsequently became a certified real property administrator.

Ms. Anne Cullather is Senior Director, Industry Affairs for Qwest's out-of-region competitive and data local exchange carrier business units, which include both Qwest Communications Corporation and Qwest Interprise America. In that capacity, she is responsible for management of incumbent local exchange carrier ("ILEC") relationships with respect to local interconnection; negotiation of all local interconnection agreements; collocation and structure access implementation and project management; and the management of public policy issues as they relate to local competition and interconnection. Ms. Cullather joined Qwest in 1997, as Director of Carrier Relations for LCI, a nationwide carrier acquired by Qwest in June 1998. In 1999, she was promoted to Senior Director of Industry Affairs for the company's competitive provider initiatives.

Prior to her employment with LCI and Qwest, she was employed for a year by a small CLEC, US ONE Communications, as Director of Carrier Relations. Prior to that position, she was employed by MCI Communications for 13 years in a variety of positions that included public policy and carrier relations responsibilities for MCI's long distance business unit, as well as with MCImetro to launch MCI's entry into the local telecommunications services arena. During her career, Ms. Cullather has testified before a number of state Commissions with respect to certification and interconnection issues on behalf of MCI, including the Commissions in Ohio, North Carolina, Georgia, Michigan,

Delaware, Virginia, Louisiana, Washington and Texas. On behalf of Qwest, she has also testified in Colorado.

PURPOSE OF TESTIMONY

Q. WHAT IS THE PURPOSE OF THIS TESTIMONY?

A. Qwest Communications Corporation ("Qwest") and its affiliates submit this testimony to assist the Department of Telecommunications and Energy ("Department") in evaluating and resolving the issues raised on January 24, 2002 in the *Order To Investigate* the security of the central offices and other facilities of Verizon Massachusetts ("Verizon"). Qwest understands the desire of federal and state agencies to review policies under their jurisdiction that could impact security "in light of heightened security concerns after the events of September 11, 2001." (*Order* at 1.) Qwest urges the Department to remain focused on the goals the Department has identified (*Order* at 1), as opposed to re-litigating past collocation security issues, such as, among other things, accidental damage to equipment, as Verizon proposes. In turn, Qwest commits to bring to this proceeding a unique perspective based on the company's competitive and incumbent local exchange businesses, as well as its prominent role in organizing efforts to protect the security of the network nationwide.

Q. WHY IS QWEST'S POSITION UNIQUE?

A. In addition to being the 4th largest U.S. long distance provider, Qwest is a competitive provider of broadband services in twenty-seven (27) markets across the country, including Massachusetts where Qwest has physical collocation (SCOPE) arrangements in twenty-seven (27) Verizon central offices ("COs"). Our corporate affiliate, Qwest Corporation ("Qwest ILEC"), succeeded the Regional Bell Operating Company US

WEST, thus becoming the ILEC throughout various western states. As the incumbent in its 14-state region, Qwest ILEC must adhere to the same Section 251 obligations in providing collocation services to competitors as Verizon does in supplying collocation space to Qwest the competitive local exchange carrier ("CLEC") in Massachusetts. Understanding security issues from both the competitive and the incumbent perspectives allows Qwest to balance the respective interests within our own corporate family in much the same way the Department will have to balance the interests of the CLEC and ILEC parties to this proceeding.

Further, in its role as an international provider of telecommunications services, Qwest has focused on the development and implementation of enhanced security of America's telecommunications infrastructure. In January of this year, Joseph P. Nacchio, Chairman and Chief Executive Officer of Qwest Communications International, Inc., accepted FCC Chairman Michael Powell's offer to chair the current term of the Network Reliability and Interoperability Council ("NRIC"), which has as one of its primary objectives to assess and address the vulnerabilities in network security as a result of terrorist activities. Then, in February, the Winter Olympics began in Salt Lake City, which was the first major international public event following the September 11 attacks. Qwest was the company responsible for planning, maintaining and supporting the heightened communications network security during the Olympic games. Finally in March 2002, Mr. Nacchio was also appointed the Co-Chairman of the National Security Telecommunications Advisory Committee ("NSTAC"), a federal advisory committee that advises President Bush on national security telecommunications matters, including wide range of policy and technical issues related to telecommunications, information

assurance, infrastructure protection and other national security and emergency preparedness concerns.

This experience developing and implementing security measures to contend with potential terrorist activities, coupled with Qwest's perspective as a CLEC and an ILEC, place Qwest in a position to highlight the tremendous flaws in Verizon's proposal for additional security measures in Massachusetts. Therefore, Qwest explains in its testimony how the proposal offered by Verizon in response to the *Order* seems to be directed more at promoting Verizon's own agenda, rather than advancing the Department's objectives.

Q. PLEASE BRIEFLY DESCRIBE THE SPECIFIC REASONING BEHIND QWEST'S OPPOSITION TO VERIZON'S PROPOSAL.

A. Verizon's Testimony neglects to mention any specific problems related to central office security arising from the threat of terrorist attacks, much less to suggest how the carriers might address such threats. Instead, Verizon chooses to address issues that have absolutely no relation to how carriers can protect the network in the face of any future terrorist activity. Segregating competitors' equipment, or eliminating physical collocation entirely in some instances, in fact, are Verizon's only actual suggested changes. In making only these suggestions, Verizon completely ignores the Department's objective to examine its collocation security policies in light of heightened security concerns after the events of September 11th, the current FCC and state regulations on reasonable security measures, and the potential effectiveness of existing security measures for ILEC premises.

In particular, Verizon's proposal fails to (1) address terrorism threats directly, (2) apply the security measures, such as background checks, evenhandedly, and (3) acknowledge and deal with the potential for Verizon's own personnel to be involved in terrorist activities at the central offices, thus rendering the proposal ineffective. Verizon makes the unsupported assumption that restricting the access of CLECs will eliminate the chances of terrorist activities in the central office. While it is true that one of the Department's purposes is "to review prior findings with respect to access by personnel of other carriers to Verizon's central offices and other facilities" (*Order* at 1), Verizon has exploited this directive by re-arguing for highly restrictive policies regarding CLEC access to central offices without any evidentiary support that the policies would improve security in light of the heightened security concerns due to the events of September 11th.

The telecommunications network is a shared environment that supports the traffic of multiple carriers, ILECs and CLECs alike. As a result, competitors have no incentive to jeopardize the network. Moreover, the existence of such overlapping networks significantly benefits all Massachusetts consumers in the event of a terrorist attack, since the availability of redundant and alternate routes should provide more alternatives to restore traffic on the network in the event of catastrophic outage. Protecting the CLEC equipment in the central office, therefore, is as essential as protecting Verizon's equipment. Furthermore, Qwest believes that neither the Department, nor Verizon, can hope to secure COs against terrorist threats by merely by restricting access by CLEC personnel. Though human action is required for terrorism, CLEC personnel, who represent only a small portion of the people accessing the COs in Massachusetts, are no

more predisposed to committing terrorism or aiding it, either knowingly or unwittingly, than are other people with CO access.

Accordingly, Qwest takes this opportunity to recommend specific approaches, which, if adopted, would ensure the adequacy of security measures implemented in central offices and other facilities in light of the heightened security concerns after the events of September 11th. Qwest's recommendations include (1) the implementation and enforcement by the Department of all existing security measures; and (2) the recognition and implementation of appropriate proposals resulting from the national government and industry groups. Though the impact of terrorism on the telecommunications network is national in scope, the Department plays a crucial role in protecting the network. Supplementing the Department's efforts with the guidelines established by the various national groups, of course, can only enhance the security in central offices and other facilities, while benefiting the consumers served by those facilities. Thus, the Department should direct Verizon to enforce the existing permissible security measures fully and fairly, while allowing the carriers to employ the definitive best practices guidelines outlined by NRIC and NSTAC for securing central offices throughout the telecommunications network.

VERIZON'S PROPOSAL FAILS TO PROTECT AGAINST TERRORISM

Q. DO THE PROPOSED CHANGES TO THE COLLOCATION SECURITY POLICY THAT APPEAR IN VERIZON'S TESTIMONY SATISFY THE DEPARTMENT'S DESIRE TO ENSURE THE ADEQUACY OF SECURITY MEASURES IMPLEMENTED AT VERIZON CENTRAL OFFICES AND OTHER FACILITIES IN LIGHT OF ANY POSSIBLE FUTURE TERRORIST THREATS?

A. No. The Department specifically requested a "presentation of evidence, which policies, if any, should be strengthened to safeguard telecommunications networks" in light of the September 11th terrorist attacks. (*Order* at 1.) Verizon presents no evidence, and avoids any discussion in its Testimony on whether the potential threat of terrorism warrants any additional security measures. Instead, the Testimony provides only a series of examples of incidents at collocation facilities—in states other than Massachusetts—that involve accidents, and thus have no relevance in protecting against terrorism. (Verizon Testimony at 3, 18, 20-23, 30-31, 33, 35-39.)

Determining whether additional measures are necessary to safeguard the central offices and other facilities against terrorism requires an in-depth analysis of all possible impacts, whether direct or indirect, that any terrorist activity at a CO may have, as well as all possible forms of terrorist activity that might transpire. Verizon in its Testimony, however, offers no such analysis. Indeed, the Verizon Testimony not only lacks any discussion of the possible methods of terrorist attacks against COs or other facilities, but also fails to discuss prospective problems arising from terrorism, or any possible means for addressing such problems. Verizon makes unsupported conclusions to justify shortsighted proposals that ultimately constitute anti-competitive security measures. (*See* AL-VZ-1-11.) As a matter of fact, there is no data in the Verizon Testimony to indicate that the security changes Verizon proposes would be effective against any particular form of terrorist attacks.

Q. DOES VERIZON PROVIDE ANY APPLICABLE EXAMPLES OF SECURITY ISSUES THAT IT HAS EXPERIENCED IN ITS CENTRAL OFFICES?

A. No. Without any examination of how to secure central offices and other premises from the threat of terrorism, Verizon argues that the collocation security measures should be heightened for reasons unrelated to threats of terrorism. For instance, Verizon bases the need for segregation and exclusion on accidental contact with another carriers' equipment. (Verizon Testimony at 3, 18, 20-23, 30-39.) In asking the Department to reexamine and strengthen existing security practices and procedures, Verizon states that current measures "alone are not enough to prevent accidents". (*Id.* at 20.) Despite the fact that the Department expressed its intent to investigate the impact of terrorism on CO security in this proceeding, Verizon continually refers to CLECs' "carelessness", "mistakes", and "inadvertant[] damage." (*Id.* at 21, 33-39.) These unsubstantiated references have nothing to do with securing the central offices and other facilities against terrorist sabotage.

Q. CAN YOU PLEASE EXPLAIN SPECIFICALLY WHY AN EXAMINATION OF CAUSES OF ACCIDENTAL SECURITY PROBLEMS IS IRRELEVANT TO DETERMINING THE NEED FOR ANY ADDITIONAL SECURITY MEASURES TO GUARD AGAINST TERRORISM?

A. Damage to CO equipment of Verizon or competitors that was accidentally caused cannot form the basis for implementing unreasonably prohibitive measures to protect against terrorism. While these incidents are certainly serious and would concern Qwest both as a collocator with equipment in another company's CO and the owner of the collocation premises, they are not intentional or criminal, let alone acts of terrorism. The Department

and the FCC have apparently taken such incidents into consideration numerous times, and rejected the general application of segregation in or exclusion from the central offices as unjust and unreasonable security measures.[1] This is, therefore, not the proper forum to re-evaluate and re-litigate the reasonable means for protecting against incidental damage to CO equipment, as Verizon proposes.

SEGREGATION AND EXCLUSION REMAIN UNREASONABLE SECURITY MEASURES

Q. ARE SEGREGATION AND EXCLUSION REASONABLE TOOLS FOR SAFEGUARDING THE CENTRAL OFFICES AND OTHER FACILITIES IN MASSACHUSETTS AGAINST TERRORISM?

A. No. Verizon erroneously contends that segregation of CLEC equipment, and exclusion of CLECs from the COs are the only forms of security than can prevent terrorist sabotage. Indeed, the central element of Verizon's proposal is that "network reliability ... can only be attained if collocators are located in separate and segregated areas of the CO." (Verizon Testimony at 27.) Verizon specifically proposes to exclude competitors from any part of the CO that contains any Verizon equipment, which is potentially the entire central office. (*Id.*) In certain "critical" central offices, Verizon would require competitors to completely surrender access to their equipment and convert to virtual collocation. (*Id.*)

Verizon makes such proposals without any explanation how potential types of terrorist activity in central offices might be mitigated by these measures. Moreover,

[1] *See Deployment of Wireline Services Offering Advanced Telecommunications Capability*, CC Docket No. 98-147, First Report and Order, 14 FCC Rcd 4761, 4785 (1999), *aff'd in part, and vacated and remanded in part sub nom. GTE Service Corp. v. FCC*, 205 F.3d 416, 425 (D.C. Cir. 2000), *on remand*, Fourth Report and Order, FCC 01-204, ¶¶ 85-104 (rel. Aug. 8, 2001)("*Collocation Remand Order*"). *See also* D.T.E. 98-57, Phase I, *Order* at 24-39, 59-62 (2000), *on recon.*, *Reconsideration Order* at 6-16, 66 (2000).

Verizon's contentions are (1) based on inaccurate assumptions that only CLEC personnel will harm the network, and that only Verizon serves critical customers; and (2) directly contradict existing state and federal law prohibiting the general application of segregation and exclusion measures.

Q. WHY IS SEGREGATION AND/OR EXCLUSION INAPPROPRIATE?

A. In essence, Verizon in its proposal incorrectly insinuates that competitors' personnel are more likely to harm the network equipment, than Verizon's own personnel. Verizon asserts that there is no way to deter terrorist acts without the ability either to segregate competitors' equipment within the central office or exclude competitors from central offices altogether. (Verizon Testimony at 23-27; *see also* AL-VZ-1-16(d).) In other words, the most effective way to protect its equipment in its COs and other premises from terrorism and sabotage, according to Verizon, is to prohibit competitors and their contractors from being in the presence of such equipment. (*Id*.)

While it is certainly true that terrorism requires human involvement in order to occur, being an ILEC does not make Verizon immune from such human factors. For example, one potential form of a terrorist threat could be a plan to get an individual or individuals into a central office to carry out terrorist tactics, such as planting a bomb to damage the network. According to Verizon, the best way to eliminate the human factor of terrorist sabotage of network facilities is to prohibit CLEC access to those facilities. What Verizon fails to explain is how such prohibition will protect against the involvement of Verizon personnel in such a scenario.

Verizon is as susceptible as any competitive carrier to hiring CO personnel that may intentionally or unintentionally aid terrorists or commit acts of terrorism themselves.

Despite Verizon's contention, the threat of being fired or disciplined directly by the ILEC is not likely to deter such persons, or those who would assist them. (*Id.* at 23.) Indeed, Verizon employment is likely to be a better guise for terrorists, as more often than not there are a greater number of Verizon personnel entering a greater number of central offices, with greater, if not full, access to areas within the CO. It is only logical, therefore, that a terrorist in a central office is more likely to be there in the guise of a Verizon employee, as opposed to any of the competitors.

Verizon's own data demonstrates that CLECs have less presence in Verizon COs than Verizon's own personnel. Almost half of Verizon's central offices in Massachusetts do not have a single competitor collocating equipment. (Qwest-VZ-1-4.) Two-thirds of the remaining COs house equipment from five or less competitors, and a third of the remaining COs only have one collocator. (*Id.*) These numbers demonstrate that Verizon currently has a significantly higher number of personnel entering central offices in Massachusetts than competitors. Moreover, the crucial areas to any CO are the main distribution frame, the power room and the switching equipment, however CLEC personnel are limited to only the areas in the Verizon COs that house CLEC equipment. The central office facilities are also branded, and generally known, as Verizon facilities. It stands to reason that because Verizon has a greater number of personnel in COs with greater access throughout the CO, that person who, intentionally or unintentionally, assists in terrorist sabotage of a central office will be a Verizon employee or contractor. Thus, with the lack of evidence from Verizon to the contrary, it is only intuitive that segregating competitors' equipment in COs is not likely to eliminate that potential avenue for terrorists attacks.

Q. IS VERIZON'S PROPOSAL BASED ON ANY OTHER MISCONCEPTIONS?

A. Yes. Verizon ultimately concludes that it is the only carrier in Massachusetts to provide service to the "critical" customers. (Verizon Testimony at 39-40.) Such an assumption leads to a bias in Verizon's proposal, which attempts only to protect Verizon's equipment. Nonetheless, competitors require the same level of protection for their customer traffic as Verizon.

While Verizon's central offices and facilities clearly perform critical and highly sensitive functions in the network, competitive carriers, such as Qwest, also serve "critical" customers, including important businesses and government agencies. In Boston and other Qwest markets, Qwest provides competitive broadband services to critical customers, including key state and federal government agencies, essential media outlets, prominent financial institutions, public utilities, universities and colleges. By Verizon's own admission, competitive carriers have become a critical part of the telecommunications network. "Indeed, based on what is undoubtedly an overly conservative estimate, CLEC fiber now reaches at least 175,000 commercial buildings (approximately one out of every four commercial buildings in the country)."[2] In addition, "[c]ompetitors (often multiple competitors) have collocated in the principal ILEC central offices serving customers of those services."[3] Competitive carriers, especially fiber providers collocating in Verizon's central offices, clearly depend on the same infrastructure as Verizon does to provide and restore service to their "critical"

[2] *Joint Petition of BellSouth, SBC and Verizon for Elimination of Mandatory Unbundling of High-Capacity Loops and Dedicated Transport*, CC Docket No. 96-98, Joint Petition at 4-5 (April 5, 2001).

[3] *Id.*

customers, and thus have great impetus to protect the Verizon equipment in a manner equal to the protection of their own equipment.

In turn, any reassessment of CO security in Massachusetts should acknowledge the need to protect competitors' equipment and facilities, as much as the measures adopted to protect Verizon's equipment and facilities. Any additional security measures must also be balanced with Verizon's obligation to provide competitors with reasonable access to the premises in accordance with the state and federal law.

Q. DOES VERIZON'S PROPOSAL TO SEGREGATE COMPETITORS' EQUIPMENT WITHIN CENTRAL OFFICES VIOLATE STATE AND FEDERAL LAW**?**

A. Yes. The FCC and the Department have found that segregation and exclusion of CLEC collocation arrangements are generally unreasonable means for securing an ILEC premise.[4] Segregation of CLEC equipment restricts the amount of space in a CO available to CLECs for collocation. Relegating CLECs to separate rooms or space may also effect the distance between the CLEC equipment and the ILEC facilities with which CLECs must interconnect. Adding to this distance increases the amount of cabling and cable racking that CLECs must purchase, as well as lengthens the CLEC facility, which may have detrimental impact on distance-sensitive services, such as DSL. These effects inevitably lead to a decrease in the number of customers CLECs can serve, not to

[4] *See supra* n. 1. The FCC prohibits incumbents from imposing segregation measure as a general policy, "particularly given the alternative means available to LECs to ensure the security of their premises." *Collocation Remand Order* at ¶ 101 *citing GTE v. FCC*, 205 F.3d at 425. The circumstances excepted from the FCC's general prohibition against segregation is if the proposed segregation measure: (a) is "available in the same or a shorter time frame as non-separated space"; (b) is available "at a cost not materially higher than the cost of non-separated space"; (c) "is comparable, from a technical and engineering standpoint, to non-separated space"; and (d) is warranted by "legitimate security concerns, or operational constraints unrelated to the incumbent's or any of its affiliates' or subsidiaries competitive concerns". *Id.* at ¶ 102. None of these criteria are met in this circumstance. For instance, Verizon's proposal suggests that CLECs must pay for any costs associated with the construction of

mention the products a CLEC can offer in a particular area in competition with Verizon. More importantly, there are numerous alternative security measures, including identification badges, background checks, electronic card key access, alarm monitoring, closed circuit television surveillance, biometric hand geometry readers, video imaging and parking restrictions, that provide efficient means of protecting carriers' equipment without artificially increasing the carriers' cost. For these reasons, it is clear that segregation in this instance contradicts the pro-competitive directives of the Department and the FCC.

Q. IS VERIZON'S PROPOSAL TO EXCLUDE COMPETITORS FROM CENTRAL OFFICES ALSO INCONSISTENT WITH STATE AND FEDERAL LAW?

A. Yes. In every central office where space for CLEC collocated equipment is exhausted, or that Verizon deems to be "critical", Verizon proposes to restrict competitors to virtual collocation. (Verizon Testimony at 22-24.) This type of restriction prevents CLECs from performing maintenance and expeditiously correcting damage for critical customers should a terrorist attack occur, and essentially limits competitors as to the equipment they may use and the services they may provide in competition with Verizon. Simply put, "driv[ing] competitors to opt for virtual collocation even though physical collocation is technically feasible, frustrat[es] the 1996 Act's preference for physical collocation."[5] In this manner, Verizon's proposal contradicts the underpinnings of the 1996 Act.

Verizon admits that its request for exclusion, as well as segregation, is "contrary to the FCC conditions". (*Id.* at 26.) Nevertheless, Verizon cites to a Wall Street Journal

---

walls or cages, however these costs alone would remove these segregation security measures from the exception to the FCC's prohibition of segregated space for CLEC equipment. Verizon Testimony at 41; *see also* AL-VZ-1-22.

[5] *Collocation Remand Order* at ¶ 93.

article and a Chairman Powell speech in Attachment 2 of its Testimony to support its argument that the current world environment requires more stringent security requirements despite its regulatory obligations under the 1996 Act. The article, when read in its entirety, actually acknowledges that, although the best means for securing critical communications is multiple providers, banishing competitors from the ILEC premises will merely proliferate Verizon's monopoly. (Verizon Testimony, Attachment 2 at 3.) Furthermore, Chairman Powell solicits concerted effort to "ensure reliability and security of our nation's communications infrastructure" (*Id*. at 11), as opposed to waiving Verizon's statutory obligations in order to enhance network security.

There is little doubt that the unsubstantiated benefit to CO security would never justify Verizon disregarding its obligations by segregating competitor equipment in all central offices, while in others excluding CLEC personnel entirely. The existence of alternatives for pro-competitive security measures guarantees that the network remains secure, yet open to competition allowing consumers in Massachusetts a choice of carriers. It is for this reason that Qwest urges the Department to reject Verizon's proposal in its entirety.

PRO-COMPETITIVE APPROACHES CAN IMPROVE CENTRAL OFFICE SECURITY

Q. DOES QWEST HAVE ANY SUGGESTIONS FOR INCREASING SECURITY AT THE CENTRAL OFFICES WITHOUT UNNECESSARILY IMPEDING COMPETITION?

A. Yes. The Department can ensure that the network receives the most complete protection possible, while also protecting the consumer marketplace against Verizon's clearly self-serving proposal. Qwest demonstrates a more productive approach for improving

security in collocation sites than the policy of exclusion and segregation pursued by Verizon. Specifically, Qwest respectfully suggests that the Department (1) require carriers to implement all existing security measures; (2) use its authority over carriers to oversee the enforcement of these security measures; and (3) direct carriers to employ the definitive guidelines established by the national government and industry groups.

The most efficient and pro-competitive means available for safeguarding the telecommunications network through CO security starts by identifying potential means for terrorist activity, and specifying the realm of possible repercussions an attack might have on a central office. Missing from Verizon's proposal, however, are the relevant security issues that would directly address actual terrorist activities. Conversely, Qwest recommends specific steps that will enhance the effectiveness of CO security in light of actual security risks associated with terrorism, such as managing access into the central office in Massachusetts.

There are infinitely more scenarios in which terrorism may impact the central offices, including many that do not necessarily involve a terrorist obtaining access to the inside of a central office. All such scenarios are currently being identified and addressed by two national government and industry groups, NRIC and NSTAC. NRIC and NSTAC provide an effective opportunity to consider the possibilities comprehensively, while identifying the sorts of terrorist threats that exist, the potential repercussions of those threats, and the security measures that would address those threats. Despite the significant efforts that national industry groups are undertaking to address the sensitive issues of protecting the network, and specifically the central offices, against terrorism, the Department has the principal responsibility to ensure that these national guidelines, not to

mention the existing security measures, are fully implemented in a manner that best protects the consumers in Massachusetts.

Q. ARE THERE STEPS THAT THE DEPARTMENT CAN TAKE TODAY TO PROTECT THE CENTRAL OFFICE?

A. Yes. Prior to imposing additional measures on competitors, the Department should determine how and whether existing security measures are sufficient to prevent damage to the telecommunications infrastructure. Verizon's interconnection agreements with carriers, such as Qwest, provide for an assortment of security measures and enforcement capabilities that could be effective without contravening the law. (Attachment 1.) Indeed, Verizon explains that there are 948 physical collocation arrangements in 169 COs in Massachusetts (Verizon Testimony at 41), yet Verizon does not have a single incident of CO security breach to report in Massachusetts. (*Id.* at 21.) By those numbers alone, the existing security measures appear to be working quite well at least with regard to routine security concerns, regardless of whether the collocation arrangements are caged or cageless. Furthermore, the Department has determined that all of the security measures listed in Attachment 1 of Verizon's Testimony are reasonable pursuant to state and federal regulations. Verizon's choice of segregation and exclusion is generally not.

Verizon provides no evidence to support the contention that current CO security measures are inadequate. More importantly, the Department expressly states that "Verizon has the burden to show that the additional security measures provide a necessary security benefit to justify added costs imposed on CLECs."[6] Prior to suggesting additional expensive and restrictive security measures (Verizon Testimony at

41), Verizon should be called upon to show that current security measures have been fully implemented, and actively monitored. It is clear that existing security measures and enforcement capabilities are not being appropriately utilized in Verizon's central offices in Massachusetts. If existing security measures are executed completely and correctly, the level of security would drastically increase without unduly burdening competitors both operationally and financially.[7]

Q. WHAT IS QWEST'S BASIS FOR THIS STATEMENT?

A. Qwest has considered the security risks associated with the extent and nature of appropriate access by personnel of other carriers to Verizon's central offices and other facilities for accessing collocation sites, and concluded that existing security measures, if utilized properly, significantly reduce the security risk. The two ways Qwest identified that can reduce the security risks associated with carrier personnel accessing a network premises, such as a central office, are to register the personnel accessing the premises and to monitor the means by which those personnel access the premises. Adequate registration of the carrier personnel requires thorough background checks of personnel entering the central offices, and computerized registration of the identification badges issued. Closely monitoring the access to the central office entails installing card readers in COs across the Massachusetts footprint, combining personnel ID badges with their electronic access cards, conducting centralized camera surveillance, and supporting these measures with consistent enforcement. These suggestions, of course, are not an

---

6 D.T.E. 98-57, *Reconsideration Order* at 13.

7 *See supra* n. 4; Attachment 1.

exhaustive list of ways Verizon can improve on its tracking of personnel allowed into the central office, and monitoring the personnel upon their arrival at the central office.

Q. HOW MIGHT ADEQUATE REGISTRATION OF CARRIER PERSONNEL INCREASE CO SECURITY?

A. Registering carrier personnel adequately allows personnel to undergo screening prior to gaining access to COs, and provides the ILEC with a list of what personnel have authorization to be in which buildings. Initially, like Qwest ILEC, Verizon could use a computerized system to issue and track identification badges upon completion of the background check. Comprehensive screening also helps to identify those personnel with criminal records, and possibly other suspect background characteristics. In fact, many large companies, such as Qwest, currently conduct background checks as part of their corporate compliance programs, premised upon the due diligence factors that describe a comprehensive compliance program according to the Federal Sentencing Guidelines for Organizations. Qwest also understand that NRIC has initiated an effort to uniformly address the issue of more stringent background checks as the national level, including a database that would store information about carrier employees.

According to Verizon, the process that Verizon contemplates requiring of competitors is consistent with the process it applies to its own employees. (Verizon Testimony, Attachment 2 at 3; Qwest-VZ-1-24.) The only regulatory restriction is that the pre-screening of collcated carrier personnel must be no more expensive or burdensome than the more stringent pre-screening and background checks Verizon says it now conducts for its own employees and contractors. Yet, Verizon does not currently require its own contractors to submit to any screening or background checks. (Qwest-

VZ-1-24.) Furthermore, Verizon requires Qwest personnel applying for identification badges and access cards to central offices to provide Verizon with authority to perform background checks. Verizon's own application for a non-employee ID Badge indicates that failure to sign such approval for a background check could result in the denial of the badge, and thus denial of access to the central offices.

Requiring competitors to subject their contractors to pre-screening requirements without subjecting Verizon's own contractors to such requirements clearly violates the nondiscrimination requirements under state and federal law. More importantly, the inconsistencies must be reconciled in order to ensure that CO security is truly effective, as well as to guarantee that all carrier personnel are being treated the same. Once this reconciliation occurs, compelling all carriers, ILECs and CLECs alike, to conduct comprehensive background checks and pre-screening prior to permitting them access to the central office as carrier personnel can enhance the effectiveness of the security measure considerably.

Q. PLEASE ALSO EXPLAIN QWEST'S SUGGESTION ON HOW VERIZON MIGHT MONITOR ACCESS INTO THE CENTRAL OFFICE MORE CLOSELY.

A. Securing any ILEC central office requires taking advantage of technology to monitor access into the central office. Installing card readers in all premises, in place of undetectable key entry, will enhance the effectiveness of CO security. Qwest ILEC continuously evaluates its security measures at its collocation facilities in its 14-state region. Consequently, Qwest ILEC has replaced key entry access with electronic card reader systems in a vast majority of its central offices. In contrast, only 15% of Verizon's COs in Massachusetts utilize electronic card readers. (Qwest-VZ-1-4, 1-20.)

Q. ARE CARD READER SYSTEMS INFALLIBLE?

A. No. Qwest is not asserting the electronic cards are infallible, though cards do provide a higher level of security than keys, which are not easily trackable, and can be duplicated. In fact, Qwest agrees with Verizon's Testimony that the biggest remaining problem with electronic card entry is the undetected misappropriation of access cards. (Verizon Testimony at 20.) Ensuring that all lost and stolen cards are reported, and that all unused cards are returned can obviously be difficult, but Verizon does not seem to be using any mechanisms available to protect against misappropriation of cards. Verizon does not keep track of which of its employees have keys to the various 240 central offices in Massachusetts (Qwest-VZ-1-23), much less how many electronic access cards it has issued in Massachusetts, or to whom those cards were issued. (AL-VZ-1-6.)

There are, however, more effective means for guarding against undetected misappropriation of cards than segregation and exclusion. First, Verizon could track the electronic access cards issued, like the Qwest ILEC tracks the access cards by incorporating the card into the personnel's ID badge. By issuing and recording the badge on its computer system, Qwest can quickly ascertain what personnel have access to which premises. Moreover, it is simple to determine whether the person with the ID badge/access card is the proper owner of the access card.

This is especially true when coupled with additional centralized camera surveillance. Remote monitoring and central storage of video files using the adequate hard drive space and proper compression techniques allows almost immediate access to remotely captured video. Several manufacturers offer products that use an Internet Protocol to transmit the data, so the video may be viewed anywhere there is IP access.

Any forced entry into the central office can display the image that caused the alarm to appear automatically on the screen of the person monitoring the video. There is also an audio feature in some models that allows the person monitoring the video to speak and listen to a person near the camera. In the case of transmission failure, the local recorder has memory for about 30 days for after-the-fact investigations.

Another potential solution to promote appropriate use by both ILEC and CLEC personnel is enforcing the obligation to return all unused cards or report all stolen or lost cards immediately. Enforcement can be easily achieved through revocation of a carrier's ability to enter a premise, inactivation of all unused cards after a specific period of time, or imposition of a fine for failure to report all missing cards. The effectiveness of the security measure should significantly increase with some form of registration efforts, and stricter enforcement, regardless of the carrier.

FEDERAL INITIATIVES CAN ENHANCE THE DEPARTMENT'S OBJECTIVES

Q. ARE THERE ANY SECURITY MEASURES THAT ARE UNFAILINGLY PREVENTIVE AGAINST ANY IMPACT FROM TERRORIST ACTIVITY?

A. Absolutely not. Despite Verizon's contentions (Verizon Testimony at 18-20), no measure can "prevent" against all security breaches, especially those associated with terrorism. Network security issues, in particular collocation security measures, in light of potential terrorist activity are, however, being efficiently and effectively resolved through federal industry initiatives. As the Hearing Officer recognized, these entities are addressing broad issues of network security, however it is also important to note that their objectives also explicitly include establishing definitive guidelines for making central offices secure from terrorism. *Ruling on Motion of AT&T, et.al.* at Part IV.

Industry collaborations allow the free-flowing exchange of ideas between all of the interested parties across the country needed to safeguard the telecommunications network from terrorist activity. Because collaborative industry efforts work so well, two different industry organizations established at the federal level, NRIC and NSTAC, have dedicated their efforts this year to resolving the precise issues that the Department has raised in this investigation. Likewise, many of the parties to this proceeding take active roles in both NRIC and NSTAC.

NRIC gives telecommunications industry leaders the opportunity to offer recommendations to the FCC and to the industry that, if implemented, would under all reasonably foreseeable circumstances assure optimal reliability of the public telecommunications networks. NRIC's members are comprised of senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations and government-related associations. According to its current Charter, the primary objective in this term of the Council is to "assess vulnerabilities in the public telecommunications networks", and "determine how best to address those vulnerabilities to prevent disruptions that would otherwise result from terrorist activities".[8] NRIC plans to conduct a survey of *all* of the carriers current practices, and issue a report by the end of 2002 that identifies the security problems, describes the best practices of the carriers, and supply checklists to be followed to prevent disruptions of the public telecommunications network.

[8] CHARTER OF THE NETWORK RELIABILITY AND INTEROPERABILITY COUNCIL (Jan. 2, 2002).

NSTAC, in turn, provides advice and analysis to the President and other government officials on matters of national security such as how to safeguard the nation's telecom infrastructure and protect critical information. NSTAC is a group of chief executive officers, and other representatives, from thirty telecommunications and technology companies. Specifically on NSTAC's present agenda is to explore the vulnerabilities of the public telecommunications network over the next three months by sharing information to address security concerns about carriers' personnel access into collocation facilities. Part of this exploration includes (1) prioritizing the physical facilities and premises in the network which may require additional security measures, (2) reviewing the process for clearing access for carriers' personnel into collocation facilities, and (3) examining the security related to equipment in collocation facilities.

Q. IS IT IMPORTANT FOR THE DEPARTMENT TO ACKNOWLEDGE THE EFFORTS OF NRIC AND NSTAC?

A. Yes. These collaborative settings are likely to be more productive than re-litigating current security measures on a state-by-state basis, as Verizon proposes to do.

It is in the public interest to encourage the most exhaustive list of appropriate security measures to guard against terrorism in the central offices. The more parties to a discussion, the greater number of issues raised and solutions proposed. The wide variety of industry players involved in NRIC and NSTAC include a significant majority of the parties participating in this proceeding, such as Qwest, Allegiance, AT&T, Covad, Sprint, Verizon, and WorldCom, not to mention representative associations, like Communication Workers of America and National Association of Regulatory and Utility Commissioners ("NARUC"). Indeed, NRIC and NSTAC commands the attention of high ranking

executives at these companies, like Qwest's CEO Nacchio and both of Verizon's key executives, Charles R. Lee and Ivan Seidenberg.

This level of participation in NRIC and NSTAC demonstrates that the security analysis not only will tend to be more exhaustive than this investigation by the Department, but will produce more objective and effective safeguards for protecting the network against terrorist activity. Since this type of collaboration tends to suggest more solutions to the problems raised, there is significant potential for the Department to create inconsistencies with the national guidelines, if the Department decides to proceed with re-litigation of reasonable security measures in Massachusetts, as Verizon proposes. Furthermore, the safeguards proposed by NRIC and NSTAC would be more objective than litigation in this proceeding, because the solutions have been adequately balanced by numerous industry players with other industry factors, and do not result from the compromises made in a litigious environment. The national industry groups remain unencumbered by the constraints of litigation. Removing compromised positions on appropriate safeguards against terrorist activity in the central offices considerably increases the chances that those safeguards remain in the best interest of Massachusetts consumers.

The national consensus reached by NRIC and NSTAC on the appropriate means for protecting against terrorist activities, therefore, should be acknowledged by the Department and implemented by carriers in Massachusetts. It is through this endeavor by the Department that Massachusetts consumers will be guaranteed the most reliable telecommunications network possible in case of any future terrorist activity. For these reasons, Qwest urges the Department to reject Verizon's proposal in its entirety, require

the carriers to implement and enforce the existing security measures fully and fairly, and direct all Massachusetts carriers to implement any further security measures established by NRIC and NSTAC.

Q. DOES THIS CONCLUDE YOUR TESTIMONY?

A. Yes, it does.